(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 187 448**
B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication of patent specification: 30.01.91

(51) Int. Cl.[5]: G 07 F 7/08, G 06 K 19/08

(21) Application number: 85307877.2

(22) Date of filing: 31.10.85

(54) Authenticator, processor and method for verification of document substance and content.

(30) Priority: 31.12.84 US 687708

(43) Date of publication of application:
16.07.86 Bulletin 86/29

(45) Publication of the grant of the patent:
30.01.91 Bulletin 91/05

(84) Designated Contracting States:
AT BE CH DE FR GB IT LI LU NL SE

(56) References cited:
EP-A-0 158 167
FR-A-2 563 351
GB-A-2 086 630
US-A-4 013 894
US-A-4 034 211
US-A-4 094 462

(73) Proprietor: LIGHT SIGNATURES, INC.
6171 West Century Boulevard
Los Angeles California 90045 (US)

(72) Inventor: Goldman, Robert N.
157 Lanipo Drive
Kailua Hawaii 96734 (US)

(74) Representative: Coles, Graham Frederick
Sommerville & Rushton et al
11 Holywell Hill
St Albans Hertfordshire AL1 1EZ (GB)

Courier Press, Leamington Spa, England.

EP 0 187 448 B1

Description

This invention relates to authenticator devices that are of the kind which carries information in a visual format and which includes a sheet of a medium that has variable translucency from one location to another of the sheet, and a machine-readable record of representations of said translucency as previously sensed at identified locations of the sheet. The invention also relates to authenticating methods and processors for such devices.

Authenticator devices of the above-specified kind, and methods and processors for authenticating them, are known for example from WO—A—8200062. Two forms of such authenticator device and both involving a paper sheet that carries printed information, are described in detail in WO—A—8200062, one a product tag or label, and the other an identification card. In each case, representations of translucency of the paper sheet at identified locations are recorded on the device itself, in the case of the tag in printed form, and in the case of the identification card in a magnetic stripe. The authenticity of the device is checked by comparing fresh sensings of the translucency at the identified locations of the sheet, with the recorded representations as read out from the record.

Authentication carried out in this way is effective for verifying that the authenticator device is genuine, but there is the problem that it may not always be effective to detect situations in which the printed or other visual information carried by the device has been modified.

It is an object of the present invention to provide an authenticator device, and an authenticating method and processor, that enable this problem to be overcome, or at least reduced.

According to one aspect of the present invention, an authenticator device of the said above-specified kind is characterised in that the recorded representations are combined in the machine-readable record with data related to a previously sensed state of said information.

Many forms of authenticator device are used to provide data of financial, commercial or legal significance. For example, stock certificates and other forms of financial paper provide a record of ownership, but also carry significant or critical information concerning that ownership. A stock certificate might designate a certain individual as the owner of a specific number of shares in an identified company, and relate such data or information to a specific certificate number. The present invention enables the provision of a certificate or other authenticator device that is capable of being readily authenticated as to both its genuineness and the information it carries.

In the latter respect, and moreover according to another aspect, the present invention relates to a method of authenticating an authenticator device of the said above-specified kind, in which representations of said translucency as sensed at identified locations of the sheet are read from the machine-readable record of the device and are compared respectively with translucency representations freshly sensed at said locations, and in which indication of authenticity of the device is provided in dependence upon the result of the comparison. According to this aspect of the present invention, the method is characterised in that data which is combined with the read-out representations in the machine-readable record is also read out and compared with data freshly-derived from the said information carried by the device, and that the provision of said indication of authenticity is also dependent upon the result of this latter comparison.

With this method there is the advantage that the indication of authenticity is dependent on both comparisons, and so in a simple manner can provide verification both as to the genuineness of the device and the information it carries.

At least one of the locations where translucency is sensed, may, with advantage, lie within a region of the sheet that contains indicia representing the said information, such that the representation of sensed translucency at this location is affected by at least one of the indicia. This representation of translucency will thus be related both to the translucency of the sheet and to at least part of the information content. The comparison between the freshly-sensed and recorded representations of translucency may in this case reveal whether there has been interference with the information and/or the substance of the device. This, then, provides added, supplementary safeguard to that afforded by the comparison between the freshly-derived and recorded data.

As a further safeguard, the translucency-representations and the data read out from the machine-readable record may be in encrypted form, and may then be submitted to decryption before they are compared with the freshly-sensed representations and freshly-derived data respectively.

According to a further aspect of the present invention there is provided a processor for authenticating a device of the said above-specified kind, which includes reading means for reading out the said translucency representations from the machine-readable record, sensing means for freshly sensing the translucency representations at said identified locations of the sheet, and comparator means for comparing the freshly-sensed translucency representations with the read-out translucency representations to provide an indication of authenticity of the device in dependence upon the result of the comparison, and which is characterised in that the processor also includes means for sensing said information carried by the device to derive data freshly in accordance therewith, and that the reading means reads out from the machine-readable record data combined with the read-out translucency representations, and that the comparator means compares the freshly-derived data with the read-out data and provides said indication in

dependence upon the result of this comparison as well as upon the result of the comparison between the freshly-sensed and read-out translucency representations.

The machine-readable record may be recorded in a magnetic stripe of the device, and in this case the said reading means may be a magnetic-stripe reader. An optical reader may be used for sensing said information from the device.

An authenticator device, and a method and processor for authenticating such a device, all in accordance with the present invention, will now be described with reference to the accompanying drawing, in which:

Figure 1 is a plan view of the authenticator device;

Figures 2 and 3 are sectional views taken on the lines 2—2 and 3—3 respectively of Figure 1;

Figure 4 is a fragmentary view of a recording format of the authenticator device of Figure 1;

Figure 5 is a block diagram of a system for producing authenticator devices of the form shown in Figure 1; and

Figure 6 is a block diagram of a processor for authenticating the authenticator device of Figure 1.

Document media, data formats, and operating systems structured in accordance with the present invention, may be embodied in a wide variety of forms, some of which may be quite different from those of the disclosed embodiment. Consequently, the specific structural and functional details disclosed herein are merely representative; yet in that regard, they are deemed to afford the best embodiment for purposes of disclosure and to provide a basis for the claims herein which define the scope of the present invention.

Referring initially to Figure 1, an illustrative document is represented in the form of an identification card for a specific individual. The card C is a laminate article incorporating a basic sheet, e.g. a bond paper sheet 15 (see Figures 2 and 3) along with certain other media functional in verification operations as explained in detail below.

The format of the card C accommodates personal identification for authorization and may, for example, be embodied as a driver's license. Of course, aspects as disclosed herein may be readily adopted for use in a wide variety of documents as indicated above including passports, valuable paper, financial cards and so on.

In the illustrative form, the card C carries print 16 (upper left) indicating the name of the assigned holder along with a photographic likeness 17 (right). The print 16 and the likeness 17 may be variously deposited on the sheet of bond paper 15 (Figure 3).

The genuineness of the card C is manifest by an individual characteristic of the card. Specifically, the card C is unique by reason of the opacity pattern of the paper sheet 15. Such an individual uniqueness characteristic may be utilized to provide signals for registration and comparison with similar data from subsequent observations. Exemplary detailed formats and structures for such sensing and comparison of a uniqueness characteristic are disclosed in United States Patent 4,423,415, Non-Counterfeitable Document System. In relation to the present invention, it is important to appreciate that the card C embodies a substantially unique, machine-readable, anti-counterfeit characteristic. In the disclosed embodiment, the uniqueness characteristic involves the document content in different ways. That is, the print 16 and the likeness 17 alter the opacity or translucency of the bond paper sheet 15 in certain specific areas. Consequently, overlays, erasures, or other modifications of the print 16 or the likeness 17 will tend to alter the translucency of the paper sheet 15 at the points of alteration. Accordingly, a preliminary safeguard is provided with respect to changes of the statistical data represented by the print 16 and the likeness 17.

In addition to the print 16 and the likeness 17, the card also carries data recorded on a magnetic stripe 18 which is affixed to the card in a conventional fashion. The magnetic stripe 18 records: clock signals, any of a variety of statistical data, and encrypted composite data for verifying the authenticity of the card C both with regard to substance and content. Specifically, character uniqueness data (indicating a genuine card C and not a counterfeit) is combined with critical statistical data to provide composite data which is encrypted and recorded on the magnetic stripe 18. That encrypted data is subsequently sensed, decoded and separately compared with freshly sensed, similar data to manifest: (1) that the card C is the genuine article, and (2) that the critical statistical data on the card has not been modified. Such verification establishes the credibility of the critical data to a level where it may be used for reliable direct input to a machine processor.

Pursuing an exemplary format of a card C as a driver's license, the document is often used for ancillary identification. For example, a driver's license often is used to confirm that a person has attained maturity, and accordingly, may legally enter into various transactions. In that regard, the print 16 states the assigned holder's name, "John J. Jones", his birthdate, "12-07-52", and an additional element of arbitrary statistical data, "JIE". In accordance herewith, the critical data comprising the birthdate in the form of printed intelligence is verified to be unaltered on the basis of two separate and distinct tests.

One test to verify that the birthdate has not been modified is involved with the uniqueness characteristic of the card C. In that regard, data locations D1, D2, D3 and D4 (Figure 1, each indicated by an "X") are designated as the test locations at which the translucency of the card is machine sensed to provide a unique anti-counterfeit characteristic. The location D3 superimposes the critical data of the birthdate to monitor that location. A second test involves data which is merged with uniqueness data then encrypted to a complex form. Such data is tested

with freshly sensed data after being decoded and segregated.

In view of the above preliminary explanation of functional aspects of the card, consider now its composition details by referring somewhat simultaneously to Figures 1, 2 and 3.

The paper sheet 15 in the card C has a reliably repeatable, machine-readable characteristic, e.g. variation in opacity. To observe an example of such a uniqueness characteristic it is simply necessary to hold a sheet of bond paper before a light source and notice the considerable variation in the opacity pattern. That characteristic has been recognized as an effective basis for anti-counterfeit uniqueness data as disclosed in detail in the above-referenced patent 4,423,415.

The paper 15 comprises the core of the card C and extends over the full area of the card. While bond paper has been determined to possess an effective uniqueness characteristic, various other materials and structures have also been recognized to possess the requisite characteristic.

The full area of the card C is also occupied by a pair of external, clear plastic sheet laminates 19 and 20. In addition to sealing the paper sheet 15, the laminate 20 also carries the magnetic stripe 18 as shown. In general, techniques for the production of laminate identification cards incorporating printed material and magnetic stripes are very well known in the art.

At this juncture, identification of specific data elements and the similarly identified representative signals will be helpful. Accordingly, the following designations are used herein:

CS—clock pulses for timing operations recorded on the stripe 18

CW—Encrypted data recorded on the magnetic stripe 18 and decodable to provide the following:

AL—Location of character uniqueness data, designating locations D1, D2, D3 and D4 (Figure 1)

CC—Uniqueness character data, sensed from locations D1, D2, D3 and D4 (Figure 1)

SD—Critical statistical data, representing the birthdate of printing 16 (Figure 1)

CC'—Freshly sensed uniqueness character data sensed from locations D1, D2, D3 and D4

SD'—Freshly sensed critical statistical data representing the birthdate of printing 16 (Figure 1)

DS—Miscellaneous statistical data, generally not of a critical nature

ta—tx—Timing signals defining specific operating states

Referring now to Figure 4, a fragment of the magnetic stripe 18 is represented. The first section 22 (left) of the magnetic stripe 18 carries data to initialize the sensing operation by a magnetic stripe reader. Such formats and the techniques associated with them are well known in the art. Accordingly, an initializing section 22 occupies the leading edge of the stripe 18 (left as illustrated).

Following the initializing section 22, the lower portion of the stripe 18 records clock pulses CS in a track 24 while the upper portion records data in a track 26. The use of recorded clock pulses to synchronize and control data flow is well known in the art.

An initial portion 28 of the data track 26 carries miscellaneous statistical data DS. Such data may take a variety of forms, as information of general or supplemental interest regarding the card C as a document. The magnetically recorded statistical data DS may be redundant, including the name of the assigned holder of the card, his birthdate, his account number, and any of a variety of other information.

Following the portion 28 of the magnetic stripe 18, a portion 30 records enclypted data CW which is derived from and is reconstructable to manifest component data including: address data AL (specifying locations D1, D2, D3 and D4), counterfeit characteristic data CC, and critical statistical data SD.

Commenting on the data signals, the uniqueness characteristic data CC actually manifests the signal levels (scale of ten) sensed at the locations D1, D2, D3 and D4 indicated on the card C. The critical statistical data SD represents the birthdate "12-07-52" of the assigned card holder as indicated by the printing 16 (Figure 1). The data CC and SD are designated by prime marks, e.g. CC' and SD' when sensed later for comparison with data from the magnetic stripe, i.e. data CC and SD.

Preliminarily, consider an exemplary use of the card C by a holder presenting the card to establish that he has attained his maturity. The magnetic stripe would be sensed to provide encrypted signals CW. The signals CW would be decrypted to provide the address signals AL, the uniqueness characteristic signals CC, and the critical statistical data SD. The address signals AL designate the locations D1, D2, D3 and D4 which are sensed to provide freshly sensed signals CC'. Also, an optical reader senses the critical statistical data SD' representing the birthdate or it is provided by manual input. Test comparisons are then performed for the signals CC with CC' and SD with SD'. Favorable comparisons of the data sets indicate that: (1) the substance composition of the document is genuine and (2) the critical statistical data has not been modified. Such positive results would also verify the card to the extent that the critical statistical data from the card can be accepted with reasonable certainty and used directly for machine processing.

The disclosed embodiment does not particularly treat the question of whether the person presenting the card C is its assigned holder. Of course, the photographic likeness 17 is helpful in that regard if the transaction is personally monitored. Alternatively, well known personal identification number techniques can be incorporated and used in conjunction with the disclosed embodiment.

In view of the above introductory explanations of the card C and its use, systems will now be considered for producing the card C and authenticating it in use. In that regard, reference initially will be made to Figure 5 for an explanation of a

structural system for completing the cards C in accordance with Figure 1. The raw cards would be as physically represented in Figure 1 bearing the print 16, the likeness 17, and the magnetic stripe 18; however, without the magnetic stripe recorded.

Preliminarily, it is helpful to recognize that signals from three sources are provided for recording the stripe 18. An independent input, e.g. terminal, provides the address data AL and the miscellaneous statistical data DS. The translucency of the card C is sensed at locations D1, D2, D3 and D4 to provide the signals CC. Finally, the printing 17 of the card C is sensed to provide the critical statistical data signals SD representative of the birthdate "12-07-52".

A card C (Figure 5, lower right) is symbolically represented to be received by a card mechanism 44. Essentially, various units are well known in the prior art which include control elements and have the capability of transporting, sensing and otherwise manipulating a document as the card C. Details of such a mechanism are disclosed in the U.S. Patent 4,423,415 referenced above. The card mechanism provides timing signals t, and directly involves other components as indicated by dashed lines 45. Specifically, the card mechanism 44 is integral with an optical reader 46, a terminal or data input device 47, a uniqueness characteristic sensor 48, and a magnetic recorder 49. These units sense and record the card C as it is passed through the mechanism 44. The optical reader 46 senses the critical statistical data SD, e.g. the date "12-07-52" from the card. The device 47 provides the address signals AL along with the miscellaneous statistical data DS. The sensor 48 provides the uniqueness characteristic signal CC. Processing and movements of these signals will now be considered.

The address signals AL from the device 47 are set in a register 52 along with the critical data signals SD from the reader 46 during a timing interval ta. From the register 52, the address signals AL are provided to the uniqueness characteristic sensor 48 which senses the card C at the locations D1, D2, D3 and D4 (Figure 1) providing uniqueness characteristic signals CC in a digital format. The characteristic sensing operation is performed by the sensor 48 during the interval of timing signal tb with the resulting signals CC provided to a compiling register 54 during the timing signal tc as illustrated in Figure 5. During the same interval tc, the address signal AL and the critical data signals SD are also received in the compiling register 54.

The data assembled in the register 54 (signals AL, SD and CC) is supplied to a cryptographic encoder 56 where it is merged and encoded using any of a variety of encryption techniques to provide decodable, representative signals CW. In that regard, a variety of cryptographic encoders are well known in the prior art and may be employed in embodiments of the present invention. Thus, the cryptographic encoder 56 operates during the interval of the timing signal td and supplies the signals CW representative of the data AL, SD and CC combined in a decodable format. From the encoder 56, the representative signals CW are supplied to a register 57 which also receives the miscellaneous data signals DS. The latter signals DS are provided to a register 60 (Figure 5, center right) from the input device 47 during the timing interval ta. Accordingly, such signals are ready for movement to the register 57 during signal te along with the signals CW.

During the interval of timing signal tf, the contents of the register 64 is supplied to the magnetic recorder 49 for transducing the data (CW and DS) onto the magnetic stripe 18 (Figure 1) of the card C. Accordingly, the card C (Figure 1) is completed with the magnetic stripe 18 recorded in the format of Figure 4. The card C may now be delivered to an assigned holder, i.e. one "John J. Jones", born "12-07-52" with the likeness 17 as depicted on the card C.

In use, the card C is authenticated by decoding the integrated encrypted data to provide separate component information for individual comparisons. Specifically, after decoding and separation, the anti-counterfeit or uniqueness information (data CC) is employed in a test to determine that the card is genuine. After decoding and separation, the critical statistical information (data SD) is employed in a test to verify that such information on the card has not been altered. A system for performing the authentication is illustrated in Figure 6 and will now be considered.

To sense and validate a card C (upper left), it is placed in an authenticator holder or mechanism 68 which is associated with a magnetic reader 69, a sensor 70, and an optical reader 71 (dashed lines 67).

The mechanism 68 includes means for providing the timing signal ta—tx. In cooperation with the mechanism 68, the magnetic reader 69 transduces the magnetic stripe 18 (Figures 1 and 4) to provide signals representative of the miscellaneous statistical data DS and the encrypted data CW. The signals sensed by the magnetic reader 69 are provided to a register 72 during a timing interval indicated by a timing signal ta.

Signal representations from the register 72 comprising the encrypted data CW are applied to a cryptographic decoder 74 which functions during an interval of timing signal tb to develop the signal representations AL, SD and CC which signals are placed in a register 76 during the interval of a timing signal tc. Note that the decrypted data actually consists of the address data AL, the critical statistical data DS and the uniqueness character data CC.

Recapitulating, the contents of the magnetic stripe 18 (Figures 1 and 4) is sensed by the magnetic reader 69 to provide two separate data packages in the register 72, i.e. encrypted data CW and miscellaneous statistical data DS. The encrypted data CW is supplied to the cryptographic decoder 74 which operates to load the register 76 with the separated and decoded data. The miscellaneous data DS from the register 72

remains in that location for use as will be explained below.

The address data AL from the register 76 is applied to the sensor 70 (upper right) for controlling that apparatus to observe the card C for uniqueness data at the locations D1, D2, D3 and D4 (Figure 1). Accordingly, fresh anti-counterfeiting, uniqueness character data CC' is sensed during signal td. Signals representative of the fresh uniqueness data CC' are applied to a comparator 78. Generally, the comparator 78 tests the freshly sensed uniqueness signals CC' with the previously recorded uniqueness signals CC (decoded from the encryption). The test serves to indicate the genuine substance of the card C.

The optical reader 71 senses the critical statistical data SD' providing representative signals to a comparator 79. Accordingly, in an action supplementary to confirming the genuine substance of the card, the statistical data signals are compared in the comparator 79 to verify the card content. Specifically, the optical reader 71 provides freshly sensed statistical data SD' for comparison during signal td with the originally sensed statistical data DS from register 76, e.g. the birthdate "12-07-52".

The comparators 78 (document genuine) and 79 (document content) provide approval output signals to an AND gate 81 which is also qualified by a timing signal te. On qualification, the occurrence of a high signal from the AND gate 81 indicates that the card is genuine and has not been altered with respect to the critical data. That output is applied to a display unit 83 and to a recorder 84 incorporating data processing capability. The display unit 83 indicates the validity of the card C. The recorder 84 records the fact that the card was tested and approved on a particular date. Essentially, the recorder 84 may include any of a variety of forms of bulk storage, e.g. magnetic tape, along with a control system for recording entries. Specifically in the disclosed embodiment, the recorder 84 operates during a timing interval tf to record the critical data SD on approval and in a format indicating the date of the approval. Additionally, miscellaneous statistical data from the register 72 may be recorded to identify the card C, the bearer of the card, or both. The miscellaneous statistical data DS is also supplied from the register 72 to a display unit 85 for direct viewing. Output is also to a file by gates 89 and 91.

To enhance an appreciation of the system of the present invention, consider an exemplary operation involving specific use. Assume the existence of a card as illustrated in Figure 1 assigned to one "John J. Jones" and further assume that the assigned bearer has presented the card to identify himself as a person who has attained his maturity, i.e. has reached the age of consent. Under the circumstances, assume that the card C is placed in the authenticator mechanism 68 (Figure 6) for testing.

From the magnetic stripe 18, the system provides miscellaneous data signals DS to activate the unit 85 with the display "Jones". Thus, a further identifier is provided. Independently, the magnetic stripe data specifies the locations (D1, D2, D3 and D4) of the uniqueness data, the previously sensed values of such data, and the critical statistical data, "12-07-52". For comparison, the uniqueness data and the critical statistical data are freshly sensed by the sensor 70 and the reader 71. Thus, the decoded original statistical data SD is compared with the freshly sensed statistical data SD'. In a proper situation, both would manifest "12-07-52" verifying card content in that regard. In such a situation, the comparator 79 would partly qualify the AND gate 81.

The test for card substance authenticity involves the uniqueness signals CC (from the magnetic stripe) and CC' (freshly sensed). Those signals are applied to the comparator 78. In operation, the comparator 78 may be as set forth in the above-referenced Patent 4,423,415. An adequate degree of comparison produces the high level of a binary signal to further qualify the AND gate 81. As a consequence, at timing interval te the gate 81 is qualified to activate the display unit 83 and the recorder 84. On activation, the display unit 83 manifests that the card is genuine and unaltered with respect to the critical statistical data. Accordingly, the user of the system simply observes the display 85 to confirm the assigned card holder's name and the display unit 83 to observe that the card is authentic. A reliable test is thus performed to verify the holder's age and his qualification to enter into a transaction requiring majority. To confirm the event of the test and the approval, the recorder 84 carries the statistical data if some question should develop at a future date. The recorder also may associate with other data processing apparatus that acts on the critical statistical data with the assurance that it has been verified. As illustrated, the system may be associated with processing apparatus incorporating a data file. Accordingly, the register 76 is coupled to an output line 93 through the AND gate 89. Similarly, the register 72 supplies statistical data through an AND gate 91 to an output line 95. The gates 89 and 91 are controlled by the approval signal from the gate 81 indicating that the card tests are genuine and not altered. It may therefore be seen that upon testing an authentic document, data from the document is captured for direct entry into a data file.

From the above descriptions, it may be appreciated that a system is disclosed for reliably verifying the genuine substance of a document and its content, e.g. that the document has not been altered with regard to critical data. Various forms of the system may well be adapted to process a wide variety of different documents. For example, the system may be adapted for use with financial paper which may be sensed by machine and if tested as genuine the resulting data may be processed with a good degree of reliability.

Claims

1. An authenticator device (C) which carries information (16) in a visual format and which includes a sheet (15) of a medium that has variable translucency from one location to another (D1—D4) of the sheet (15), and a machine-readable record (18) of representations (CC) of said translucency as previously sensed at identified locations (D1—D4) of the sheet (15), characterised in that the recorded representations (CC) are combined in the machine-readable record (18) with data (SD) related to a previously sensed state of said information (16).

2. An authenticator device (C) according to Claim 1 wherein said information is in printed form (16) on the sheet (15).

3. An authenticator device (C) according to Claim 1 or Claim 2 including a magnetic stripe (18), and wherein the machine-readable record is recorded magnetically in the stripe (18).

4. An authenticator device according to any one of Claims 1 to 3 wherein the sheet is of paper (15).

5. A method of authenticating a device (C) which carries information (16) in a visual format and which includes a sheet (15) of a medium that has variable translucency from one location to another (D1—D4) of the sheet (15), in which representations (CC) of said translucency as sensed at identified locations (D1—D4) of the sheet (15) are read from a machine-readable record (18) of the device (C) and are compared (78) respectively with translucency representations (CC') freshly sensed at said locations (D1—D4), and in which indication (83) of authenticity of the device (C) is provided in dependence upon the result of the comparison, characterised in that data (SD) which is combined with the read-out representations (CC) in the machine-readable record (18) is also read out and compared (79) with data (SD') freshly-derived from the said information (16) carried by the device (C), and that the provision of said indication (83) of authenticity is also dependent upon the result of this latter comparison (79).

6. A method according to Claim 5 wherein the said information is in printed form (16) on the sheet (15).

7. A method according to Claim 5 or Claim 6 wherein the device (C) includes a magnetic stripe (18), and the machine-readable record is read from the stripe (18).

8. A method according to any one of Claims 5 to 7 wherein the sheet is of paper (15).

9. A method according to any one of Claims 5 to 8 wherein at least one (D3) of said locations lies within a region of said sheet (15) that contains indicia (16) representing said information, to the effect that the representation (CC) of sensed translucency at such location (D3) is affected by at least one ("2") of said indicia (16).

10. A method according to any one of Claims 5 to 9 wherein the data derived from said information (16) carried by the device (C) is data (SD') read out from the device (C) by an optical reader (71).

11. A method according to any one of Claims 5 to 10 wherein the said representations (CC) and data (SD) are read out from the machine-readable record (18) in encrypted form and are submitted to decryption (74) before their comparison (78, 79) with the freshly-sensed representations (CC') and freshly-derived data (SD') respectively.

12. A processor for authenticating a device (C) which carries information (16) in a visual format and which includes a sheet (15) of a medium that has variable translucency from one location to another (D1—D4) of the sheet (15), and a machine-readable record (18) of representations (CC) of said translucency as sensed at identified locations (D1—D4) of the sheet (15), the processor including reading means (69) for reading out the said translucency representations (CC) from the machine-readable record (18), sensing means (70) for freshly sensing the translucency representations (CC') at said identified locations (D1—D4) of the sheet (15), and comparator means (78, 79) for comparing the freshly-sensed translucency representations (CC') with the translucency representations (CC) read out to provide an indication (83) of authenticity of the device (C) in dependence upon the result of the comparison, characterised in that the processor also includes means (71) for sensing said information (16) carried by the device (C) to derive data (SD') freshly in accordance therewith, and that the reading means (69) reads out from the machine-readable record (18) data (SD) combined with the read-out translucency representations (CC), and that the comparator means (78, 79) compares the freshly-derived data (SD') with the read-out data (SD) and provides said indication in dependence upon the result of this comparison (79) as well as upon the result of the comparison (78) between the freshly-sensed and read-out translucency representations (CC', CC).

13. A processor according to Claim 12 wherein the machine-readable record is recorded in a magnetic stripe (18) of the device (C), and the said reading means is a magnetic-stripe reader (69).

14. A processor according to Claim 12 or Claim 13 wherein the means for sensing said information (16) from the device (C) is an optical reader (71).

15. A processor according to any one of Claims 12 to 14 wherein the recorded representations (CC) and data (SD) are read out from the machine-readable record (18) in encrypted form, and the processor includes decryption means (74) for decrypting them before they are applied to the comparator means (78, 79) for comparison with the freshly-sensed representations (CC') and freshly-derived data (SD') respectively.

Patentansprüche

1. Vorrichtung (C) zum Echtheitsnachweise mit sichtbaren Informationen (16) und mit einer Folie (15) aus einem Material mit variierender Durchsichtigkeit von einer Stelle zu einer anderen Stelle (D1—D4) der Folie (15), und mit einer maschinenlesbaren Aufzeichnung (18) von Kenngrößen (CC) der Durchsichtigkeit, die an bestimmten Stellen

(D1—D4) der Folie (15) vorher ermittelt worden sind, dadurch gekennzeichnet, daß die aufgezeichneten Kenngrößen (CC) in der maschinenlesbaren Aufzeichnung (18) mit Daten (SD) kombiniert werden, die zu einem vorher ermittelten Zustand der Information (16) in Beziehung stehen.

2. Vorrichtung (C) zum Echtheitsnachweise nach Anspruch 1, wobei die Information sich in gedruckter Form (16) auf der Folie (15) befindet.

3. Vorrichtung (C) zum Echtheitsnachweis nach Anspruch 1 oder 2, mit einem Magnetstreifen (18) und wobei die maschinenlesbare Aufzeichnung auf dem Streifen (18) magnetisch aufgezeichnet wird.

4. Vorrichtung zum Echtheitsnachweis nach einem der Ansprüche 1 bis 3, wobei die Folie aus Papier (15) besteht.

5. Verfahren zur Echtheitsprüfung einer Vorrichtung (C), die in sichtbarer Form Informationen (16) trägt und eine Folie (15) aus einem Material aufweist, das von einer Stelle zu einer anderen Stelle (D1—D4) der Folie (15) eine variable Durchsichtigkeit aufweist, wobei Kenngrößen (CC) der Druchsichtigkeit, die an bestimmten Stellen (D1—D4) der Folie (15) ermittelt werden, von einer maschinenlesbaren Aufzeichnung (18) der Vorrichtung (C) gelesen und entsprechend mit Durchsichtigkeitskenngrößen (CC') verglichen (78) werden, die an den Stellen (D1—D4) neu ermittelt worden sind, und wobei eine Angabe (83) der Authentizität der Vorrichtung (C) in Abhängigkeit vom Vergleichsresultat gegeben wird, dadurch gekennzeichnet, daß die Daten (SD) die mit den ausgelesenen Kenngrößen (CC) in der maschinenlesbaren Aufzeichnung (18) kombiniert werden, ebenfalls ausgelesen und mit Daten (SD') verglichen (79) werden, die aus den auf der Vorrichtung (C) enthaltenen Informationen (16) neu ermittelt worden sind, und daß die Angabe (83) der Authentizität ferner in Abhängigkeit vom Ergebnis dieses letzten Vergleichs (79) gegeben wird.

6. Verfahren nach Anspruch 5, wobei die Information in gedruckter Form (16) auf der Folie (15) vorliegt.

7. Verfahren nach Anspruch 5 oder 6, wobei die Vorrichtung (C) einen Magnetstreifen (18) aufweist und die maschinenlesbare Aufzeichnung von dem Streifen (18) gelesen wird.

8. Verfahren nach einem der Ansprüche 5 bis 7, wobei die Folie aus Papier (15) besteht.

9. Verfahren nach einem der Ansprüche 5 bis 8, wobei mindestens eine (D3) der Stellen innerhalb eines Bereichs der Folie (15) liegt, der Kennzeichen (16) für die Information enthält, so daß die Kenngröße (CC) der gemessenen Durchsichtigkeit an dieser Stelle (D3) durch mindestens eine ("2") der Kennzeichnungen (16) beeinflußt wird.

10. Verfahren nach einem der Ansprüche 5 bis 9, wobei die von der Information (16) auf der Vorrichtung (C) abgeleiteten Daten solche Daten (SD') sind, die von der Vorrichtung (C) mit Hilfe eines optischen Lesegeräts (71) ausgelesen werden.

11. Verfahren nach einem der Ansprüche 5 bis 10, wobei die Kenngrößen (CC) und Daten (SD) aus der maschinenlesbaren Aufzeichnung (18) in verschlüsselter Form ausgelesen und vor ihrem Vergleich (78, 79) mit den neu ermittelten Kenngrößen (CC') bzw. den neu abgeleiteten Daten (SD') entschlüsselt (74) werden.

12. Prozessor zum Echtheitsnachweise einer Vorrichtung (C), die Informationen (16) in sichtbarer Form trägt und eine Folie (15) aus einem Material aufweist, das in Abhängigkeit vom Ort (D1—D4) der Folie (15) eine variable Durchsichtigkeit aufweist, und mit einer maschinenlesbaren Aufzeichnung (18) der Kenngrößen (CC) der an bestimmten Stellen (D1—D4) der Folie (15) gemessenen Durchsichtigkeit, wobei der Prozessor eine Leseeinrichtung (69) zum Auslesen der Durchsichtigkeitskenngrößen (CC) aus der maschinenlesbaren Aufzeichnung (18), eine Sensoreinrichtung (70) zum neu Ausmessen der Durchsichtigkeitskenngrößen (CC') an den bestimmten Stellen (D1—D4) der Folie (15) sowie einen Vergleicher (78, 79) zum Vergleichen der neu gemessenen Durchsichtigkeitskenngrößen (CC') mit den ausgelesenen Durchsichtigkeitskenngrößen (CC) aufweist, um eine Angabe (83) der Authentizität der Vorrichtung (C) in Abhängigkeit vom Vergleichsergebnis auszugeben, dadurch gekennzeichnet, daß der Prozessor ferner eine Einrichtung (71) zum Ermitteln der von der Vorrichtung (C) gespeicherten Information (16) aufweist, um dementsprechend neue Daten (SD') abzuleiten, daß die Leseeinheit (69) aus der maschinenlesbaren Aufzeichnung (18) Daten (SD) in Kombination mit den ausgelesenen Durchsichtigkeitskenngrößen (CC) ausliest und daß der Vergleicher (78, 79) die neu abgeleiteten Daten (SD') mit den ausgelesenen Daten (SD) vergleicht und die Angabe in Abhängigkeit von diesem Vergleichsergebnis sowie in Abhängigkeit von dem Vergleichsergebnis (78) zwischen den neu gemessenen und ausgelesenen Durchsichtigkeitskenngrößen (CC', CC) ausgibt.

13. Prozessor nach Anspruch 12, wobei die maschinenlesbare Aufzeichnung in einem Magnetstreifen (18) der Vorrichtung (C) aufgezeichnet ist und die Leseeinheit ein Magnetstreifenleser (69) ist.

14. Prozessor nach Anspruch 12 oder 13, wobei die Einrichtung zum Ermitteln der Information (16) auf der Vorrichtung (C) ein optisches Lesegerät (71) ist.

15. Prozessor nach einem der Ansprüche 12 bis 14, wobei die aufgezeichneten Kenngrößen (CC) und Daten (SD) aus der maschinenlesbaren Aufzeichnung (18) in verschlüsselter Form ausgelesen werden und der Prozessor eine Entschlüsselungseinheit (74) aufweist, um diese vor dem Zuführen zu dem Vergleicher (78, 79) zum Vergleichen mit den neu gemessenen Kenngrößen (CC') bzw. den neu abgeleiteten Daten (SD') zu entschlüsseln.

Revendications

1. Dispositif authentificateur (C) qui porte une

information (16) en une présentation visible et qui comprend une feuille (15) d'un support qui présente une translucidité variable d'un emplacement à un autre (D1—D4) de la feuille (15), et un enregistrement (18), assimilable par machine, de représentations (CC) de ladite translucidité telle que captée précédemment en des emplacements identifiés (D1—D4) de la feuille (15), caractérisé en ce que les représentations enregistrées (CC) sont combinées dans l'enregistrement (18) assimilable par machine avec des données (SD) liées à un état précédemment capté de ladite information (16).

2. Dispositif authentificateur (C) selon la revendication 1, dans lequel ladite information est sous une forme imprimée (16) sur la feuille (15).

3. Dispositif authentificateur (C) selon la revendication 1 ou la revendication 2, comprenant une bande magnétique (18), et dans lequel l'enregistrement assimilable par machine est enregistré magnétiquement dans la bande (8).

4. Dispositif authentificateur selon l'une quelconque des revendications 1 à 3, dans lequel la feuille est en papier (15).

5. Procédé d'authentification d'un dispositif (C) qui porte une information (16) en une présentation visible et qui comprend une feuille (15) d'un support qui présente une translucidité variable d'un emplacement à un autre (D1—D4) de la feuille (15), dans lequel des représentations (CC) de ladite translucidité telles que captées en des emplacements identifiés (D1—D4) de la feuille (15) sont lues à partir d'un enregistrement (18), assimilable par machine, du dispositif (C) et sont comparées (78) respectivement à des représentations (CC') de la translucidité, fraîchement captées auxdits emplacements (D1—D4), et dans lequel une indication (83) de l'authenticité du dispositif (C) est fournie en fonction du résultat de la comparaison, caractérisé en ce que des données (SD), qui sont combinées aux représentations lues (CC) dans l'enregistrement (18) assimilable par machine, sont également lues et comparées (79) à des données (SD') fraîchement déduites de ladite information (16) portée par le dispositif (C), et en ce que la fourniture de ladite information (83) de l'authenticité dépend aussi du résultat de cette dernière comparaison (79).

6. Procédé selon la revendication 5, dans lequel ladite information est sous une forme imprimée (16) sur la feuille (15).

7. Procédé selon la revendication 5 ou la revendication 6, dans lequel le dispositif (C) comprend une bande magnétique (18), et l'enregistrement assimilable par machine est lu sur la bande (18).

8. Procédé selon l'une quelconque des revendications 5 à 7, dans lequel la feuille est en papier (15).

9. Procédé selon l'une quelconque des revendications 5 à 8, dans lequel au moins l'un (D3) desdits emplacements s'étend dans une région de ladite feuille (15) qui contient des signes (16) représentant ladite information, afin que la représentation (CC) de la translucidité captée à cet emplacement (D3) soit affectée par au moins l'un ("2") desdits signes (16).

10. Procédé selon l'une quelconque des revendications 5 à 9, dans lequel les données déduites de ladite information (16) portée par le dispositif (C) sont des données (SD') lues sur le dispositif (C) par un lecteur optique (71).

11. Procédé selon l'une quelconque des revendications 5 à 10, dans lequel lesdites représentations (CC) et lesdites données (SD) sont lues sur l'enregistrement (18) assimilable par machine sous une forme chiffrée et sont soumises à un déchiffrement (74) avant leur comparaison (78, 79) avec les représentations fraîchement captées (CC') et les données fraîchement déduites (SD') respectivement.

12. Processeur pour authentifier un dispositif (C) qui porte une information (16) en une présentation visible et qui comprend une feuille (15) d'un support qui présente une translucidité variable d'un emplacement à un autre (D1—D4) de la feuille (15), et un enregistrement (18), assimilable par machine, de représentations (CC) de ladite translucidité telles que captées en des emplacements identifiés (D1—D4) de la feuille (15), le processeur comprenant des moyens de lecture (69) destinés à lire lesdites représentations (CC) de translucidité sur le support (18) assimilable par machine, des moyens de captage (70) destinés à capter de façon nouvelle les représentations (CC') de translucidité auxdits emplacements identifiés (D1—D4) de la feuille (15), et des moyens comparateurs (78, 79) destinés à comparer les représentations (CC') de translucidité nouvellement captées avec les représentations (CC) de translucidité lues pour donner une indication (83) de l'authenticité du dispositif (C) en fonction du résultat de la comparaison, caractérisé en ce que le processeur comprend aussi des moyens (71) destinés à capter ladite information (16) portée par le dispositif (C) pour déduire des données (SD') de manière nouvelle conformément à cette information, et en ce que les moyens de lecture (69) lisent sur l'enregistrement (18) assimilable par machine des données (SD) combinées aux représentations (CC) de translucidité lues, et en ce que les moyens comparateurs (78, 79) comparent les données (SD') nouvellement déduites avec les données lues (SD) et produisent ladite indication en fonction du résultat de cette comparaison (79) ainsi que du résultat de la comparaison (78) entre les représentations de translucidité (CC', CC) nouvellement captées et lues.

13. Processeur selon la revendication 12, dans lequel l'enregistrement assimilable par machine est enregistré dans une bande magnétique (18) du dispositif (C), et lesdits moyens de lecture comprennent un lecteur (69) de bande magnétique.

14. Processeur selon la revendication 12 ou la revendication 13, dans lequel les moyens de captage de ladite information (16) sur le dispositif (C) comprennent un lecteur optique (71).

15. Processeur selon l'une quelconque des revendications 12 à 14, dans lequel les représentations enregistrées (CC) et les données (SD) sont lues sur le support (18) assimilable par machine

sous une forme chiffrée, et le processeur comprend des moyens de déchiffrement (74) destinés à les déchiffrer avant qu'elles soient appliquées aux moyens comparateurs (78, 79) pour une comparaison avec les représentations nouvellement captées (CC') et les données nouvellement déduites (SD'), respectivement.

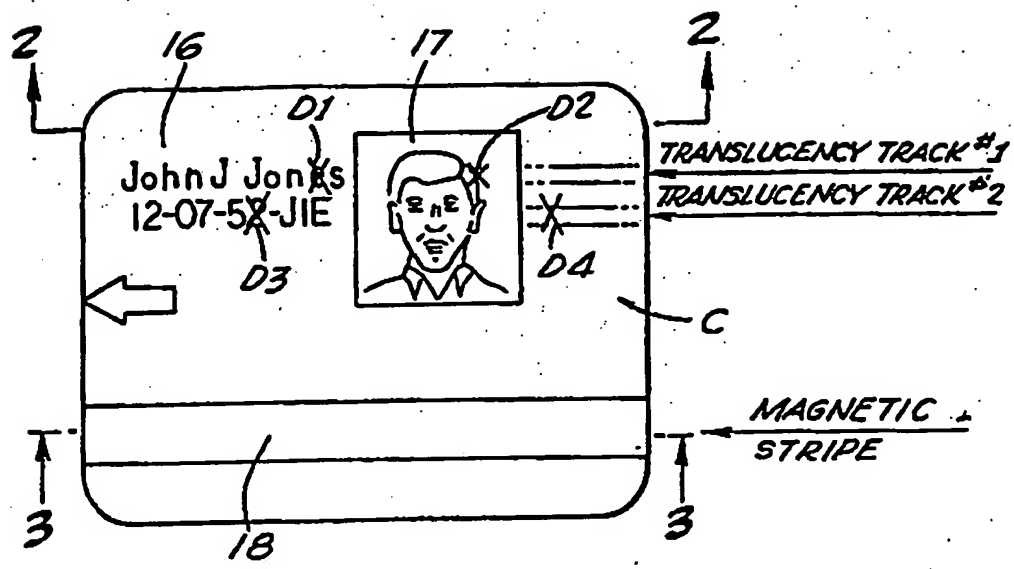


FIG. 1

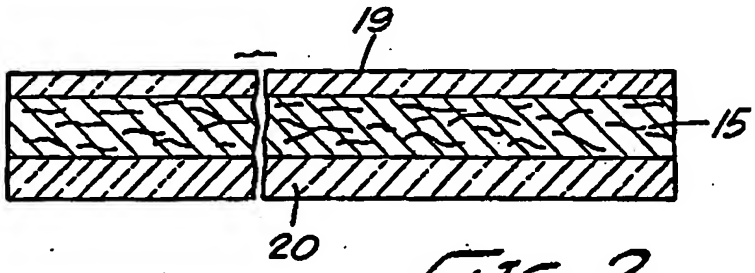


FIG. 2

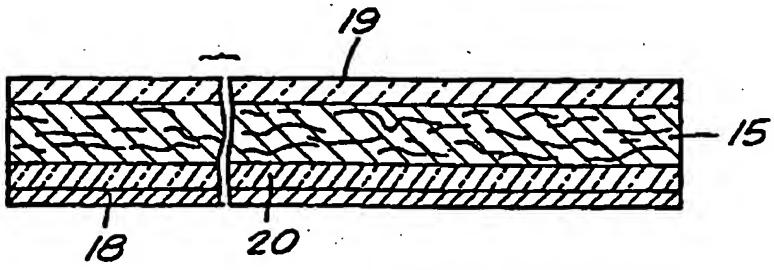


FIG. 3

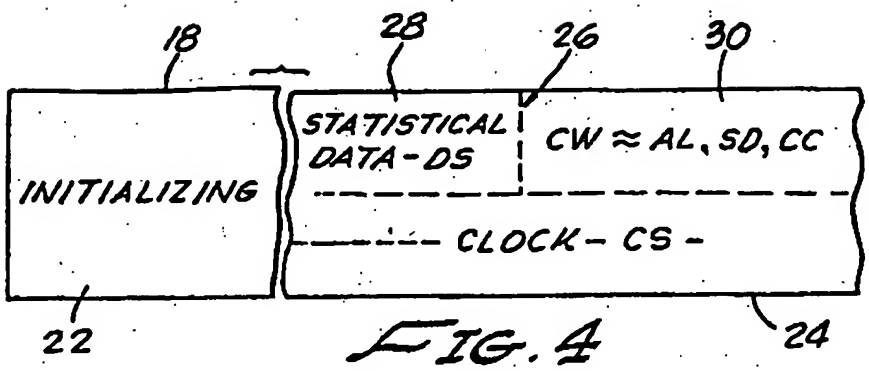

18
28
26
30
INITIALIZING
STATISTICAL DATA-DS
CW ≈ AL, SD, CC
CLOCK - CS -
22
24

FIG. 4

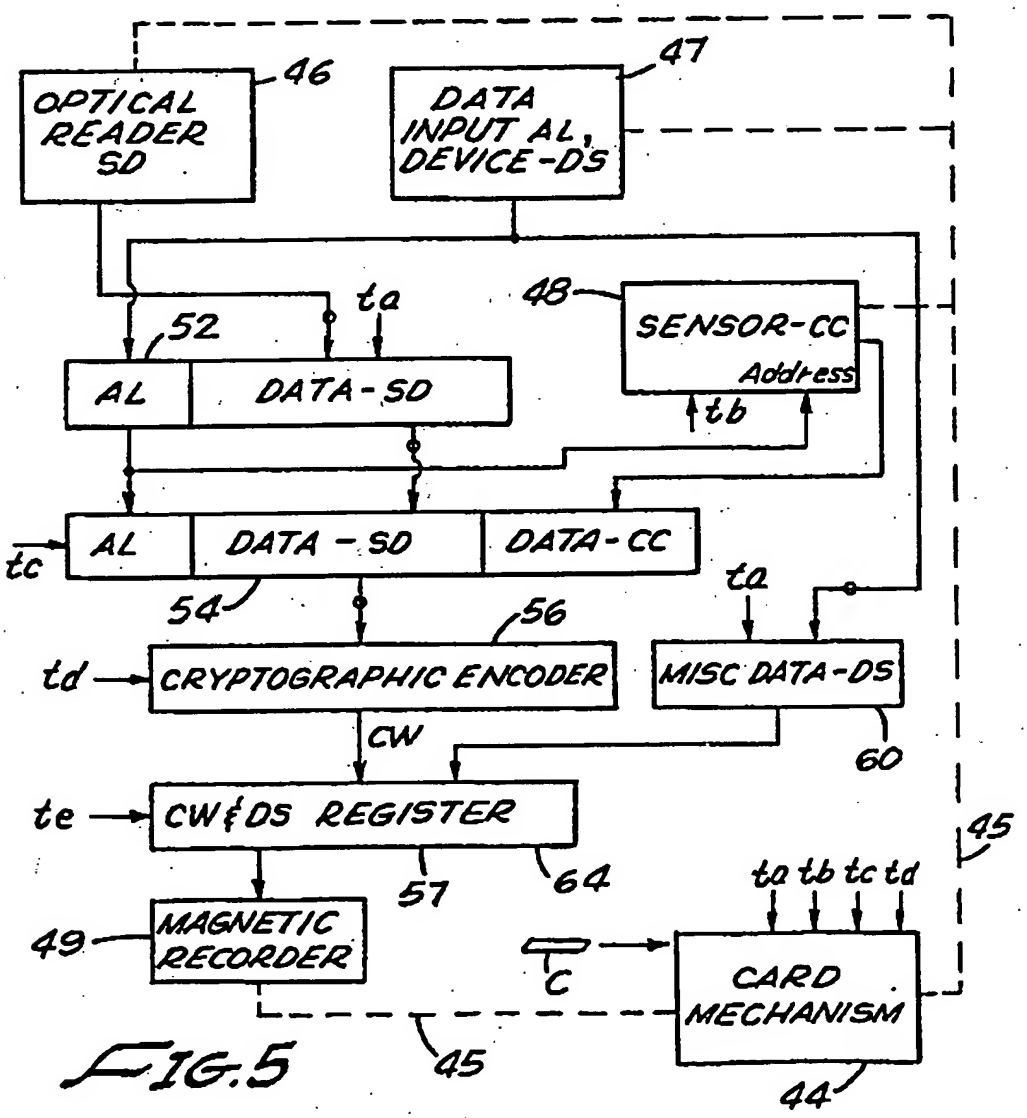
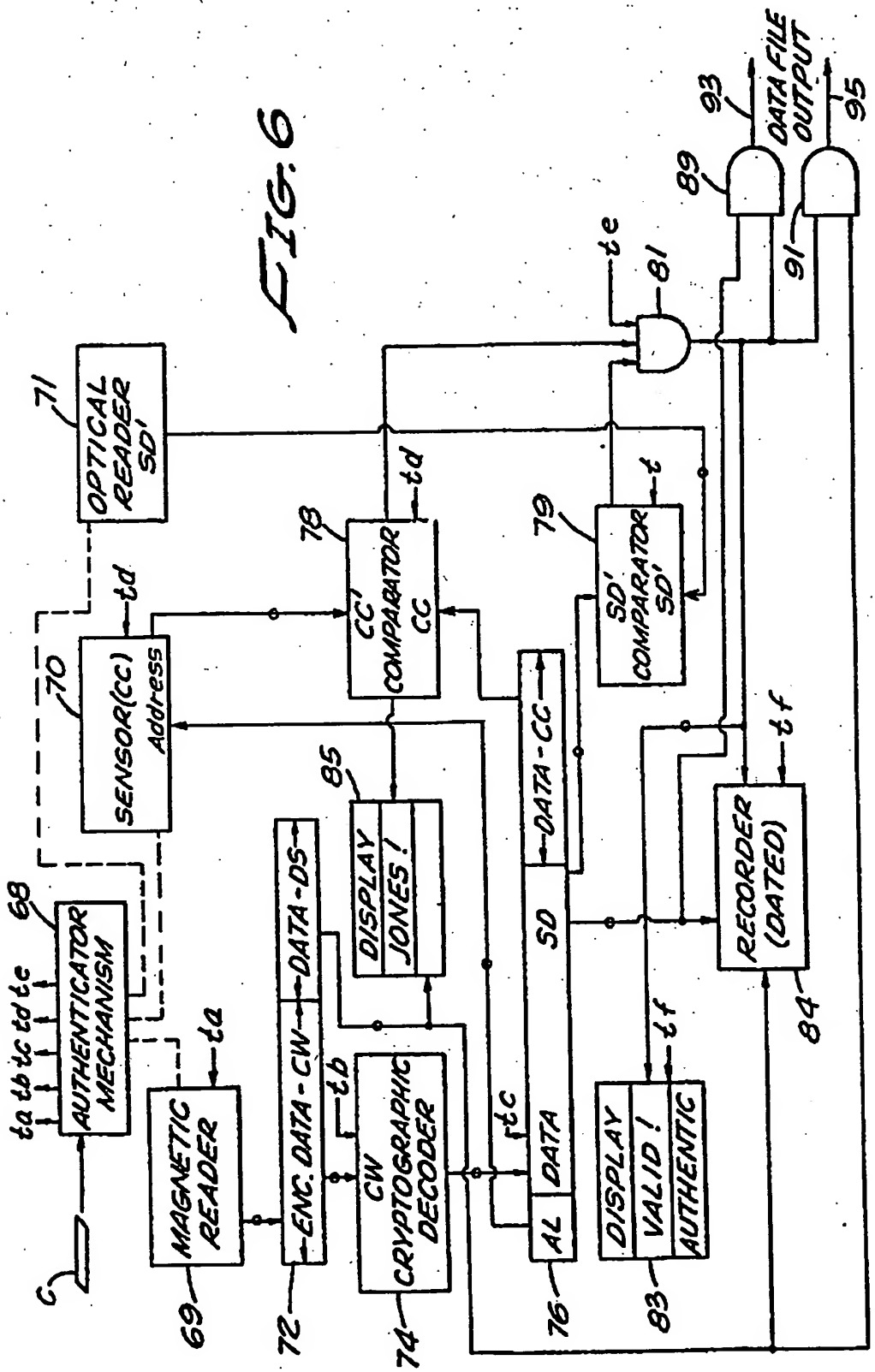

OPTICAL READER SD
46
DATA INPUT AL, DEVICE-DS
47
ta
48
SENSOR-CC
Address
52
AL
DATA-SD
tb
tc
AL
DATA - SD
DATA-CC
54
56
ta
td
CRYPTOGRAPHIC ENCODER
MISC DATA-DS
CW
60
te
CW & DS REGISTER
45
57
64
ta tb tc td
49
MAGNETIC RECORDER
C
CARD MECHANISM
45
44

FIG. 5

FIG. 6


OPTICAL READER SD'
71
SENSOR(CC) Address
70
AUTHENTICATOR MECHANISM
68
MAGNETIC READER
69
ENC. DATA - CW
DATA - DS
72
CW CRYPTOGRAPHIC DECODER
74
CC' COMPARATOR CC
78
SD' COMPARATOR SD'
79
DISPLAY JONES !
85
DATA - CC
SD
DATA
AL
76
DISPLAY VALID ! AUTHENTIC
83
RECORDER (DATED)
84
81
89
91
93
DATA FILE OUTPUT
95
ta tb tc td te
ta
tb
tc
td
te
tf